HERBERT SMITH FREEHILLS

CHINA INVESTMENTS E-BULLETIN

CHINESE VERSION | CONTACTS

China Cybersecurity and Data Protection: China updates its own GDPR – what you need to know about the changes

21 July 2020 | Greater China
Nanda Lau, Gavin Guo and James Gong

China has published revisions to the *Personal Information Security Specification* which are due to come into effect on 1 October 2020. The revised regime focuses on ensuring that the consent obtained by personal information controllers for processing personal information has been freely given, is specific and informed. In addition, new requirements are being added to enhance protection of personal information processed using new technologies, such as profiling and artificial intelligence. Compliance measures similar to those adopted by the European Union are also being introduced.

In this e-bulletin we highlight the key changes and set out our observations. We recommend that companies processing personal information in China familiarise themselves with the new regime and implement measures to comply with the requirements in good time.

BACKGROUND

In the absence of a unified national law on personal information protection, the *Cyber Security Law* (**CSL**) enacted in November 2016 serves as the main legislation that protects personal information processed on networks in China. To implement the high level principles laid down in the CSL, the *Personal Information Security Specification* (**Specification**) was first published by the State Administration of Market Regulation and the Standardisation Administration of China in December 2017. The Specification

sets out detailed requirements for the processing of personal information by personal information controllers (please click here for our bulletin).

The Specification contains recommended national standards so compliance is technically not mandatory and a breach will not necessarily give rise to legal liability. However, the Specification also guides the regulation of personal information processing activities by the regulatory authorities and so could be used as a benchmark in enforcing the personal information protection provisions in the CSL and other laws and regulations.

The non-mandatory nature of the Specification also reflects the staged approach taken by the regulators to test the requirements with stakeholders and pave the way for future mandatory legislation and standards. As a result, since the Specification was first published, it has been subject to ongoing discussion and amendment. Unusually, particularly for national standards that were only published in 2017, there have been three public consultations on revised drafts of the Specification since February 2019 culminating in the revised version which will come into effect on 1 October 2020.

Back

HIGHLIGHTS OF AMENDMENTS TO THE SPECIFICATION

I. Evolving scope of personal information and personal information subject and the principle of personal information security

The revised Specification will finally replace all references to personal data and privacy in the current version with personal information. The definitions of personal information and sensitive personal information remain unchanged. An annotation clarifies that the scope also includes information that is generated from the processing of personal information or other information, which expressly contemplates customer profiling and segmentation information.

The examples of sensitive personal information in Appendix B of the Specification have been updated, notably to remove personal telephone numbers and network identifiers, such as names, email addresses, passwords, password questions and digital certificates. Contact lists, friend lists and group lists have now been added to the scope.

The definition of personal information subject (currently referred to as personal data subject) is amended to extend the scope from natural persons identified by the personal information to also include those associated with the personal information.

Consistent with the CSL, the revised Specification makes “lawfulness, legitimacy and necessity” the general principle for processing of personal information.

II. Definitions of consent and explicit consent

The revised regime introduces a definition of consent, as meaning an act by which a personal information subject clearly authorises the processing of personal information. Consent consists of authorisation by affirmative action or by a passive act (for example where a personal information subject does not leave an information collection area after being informed of the data collection act). However, it should be noted that it may not be reasonable to presume consent by passive act in certain situations. For instance, in a video surveillance area, CCTV camera signage may not be sufficiently

conspicuous to bring it to the attention of the personal information subject. Besides, if the personal information subject leaves the area upon seeing the signage, footage may have already been collected without consent.

Authorisation by affirmative action amounts to explicit consent, which is defined in the revised Specification as explicit authorisation given by a personal information subject to personal information processing by way of an affirmative written or oral statement in paper or electronic form or a voluntary affirmative action. Oral statement (presumably by voice recording) is newly added as a valid method of giving explicit consent.

III. Elements of valid consent

The amended Specification lays down certain requirements for personal information controllers when obtaining consent from personal information subjects.

Freely given

When a product or service provides multiple business functions (ie types of service that meets the specific use or demand of a personal information subject) that collect personal information, personal information controllers should not force personal information subjects to consent to the collection of personal information against their will.

The consent must be a voluntary affirmative action, ie an explicit consent, and can be withdrawn. Specifically, a personal information subject should not be required to given a single consent to a bundle of personal information collection requests from multiple business functions of a service or product. This is similar to the concept of granularity under the General Data Protection Regulation (**GDPR**) of the European Union which provides that personal information subjects should be free to choose which purposes they accept and give separate consent when a service or product may involve multiple processing operations.

The revised Specification provides that withdrawing consent or turning off certain business functions should not result in frequent repeated requests being sent to the personal information subject or any unaffected functions being stopped or their service quality lowered. This is equivalent to the concept of detriment under the GDPR which provides for personal information subjects to be able to withdraw their consent without detriment.

However, we note that the revised Specification only expressly extends the principle of freely given consent to data processing activities where a product or service involves multiple business functions. This is a pity as it should apply irrespective of whether the relevant product or service involves single or multiple business functions.

Specific

The principle of specific purpose is amended in the revised Specification to require that the purpose for processing personal information must be specific, clear and concrete. In particular, personal information controllers must request consent for specific purposes rather than generic ones when collecting personal information for multiple business functions or purposes. Vague purpose descriptions, such as for “improvement of service quality” or “enhancement of security”, will not meet this requirement.

Informed

The revised Specification reiterates the requirement that personal information controllers must keep personal information subjects informed of the rules for processing personal information, such as the purpose, means and scope. This can be achieved through a personal information protection policy. In cases involving multiple business functions, the purpose, means and scope for each function that processes personal information must be covered.

Minimum content requirements for a personal information policy (currently referred to as a privacy policy) and how the information should be provided to obtain valid consent are also included.

Basic and extended functions

Appendix C to the revised Specification sets out a mechanism to ensure that freely given and informed consent is obtained in the context of personal information processed by multiple business functions of a service or product, especially a mobile application.

Essentially, the business functions are divided into basic functions and extended functions. Basic functions are those that if they are not provided by the personal information controller, the personal information subjects will normally not choose to use the product or service. The personal information controllers must identify the basic functions from the perspective and demand of the personal information subjects, taking into account factors relating to the product or service including: the market positioning, name, description in the application store and the categories of the app. All other functions are considered extended functions.

Explicit consent is required for both basic functions and extended functions. Personal information subjects can give their consent by a single affirmative action to data processing by all the basic functions unless it is not necessary for all of them to be turned on. For extended functions, personal information controllers are required to obtain a separate consent for each function that processes personal information.

Appendix C also provides a sample to demonstrate to mobile app operators how to design the graphical user interface to inform the users and obtain their valid consent.

The concepts of basic and extended functions replace core and non-core functions in the current Specification and extend the application from sensitive personal information to all personal information. However, these provisions have been moved from the operative provisions in the main body of the Specification to an appendix. This suggests that the regulators do not want to restrict the methods that personal information controllers can use to obtain valid consent, although they are recommended to follow the approach in Appendix C.

IV. Special requirements for profiling technologies

The amended regime lays down requirements which will apply to profiling and similar technologies commonly employed in marketing and automated decision-making functions which are enabled by processing an enormous volume of personal information.

Restrictions on profiling

The revised Specification sets out general restrictions on profiling. The segmentation description of the personal information subject in profiling should not include any

content that is (i) obscene, erotic, gambling, superstitious, terrorist or violent or (ii) discriminatory on the personal information subjects' ethnicity, race, relegation, disability or illness. [Profiling should not be used in a way that infringes a person's or organisation's legal rights and interests or, among other things, jeopardizes national security or harms social order.

Pooling and converging of personal information that has been collected for different operational purposes is also restricted. Whilst pooling and converging is not precisely defined, it appears to refer to the processing of personal information from different sources such as information collected by different personal information controllers. The revised Specification reiterates that such further processing must be within the scope of processing that has been consented to. A personal information security impact assessment must be conducted and personal information controllers must implement effective personal information protection measures.

Personalised display

Personalised display is defined as showing information or providing search results of products or services based on the browsing history, interests, purchase record or habits of a personal information subject. This appears to capture targeted marketing and displaying content based on profiling. When using personalised display, personal information controllers must:

(i) separately and distinctively show content on personalised display and content that is not, for example by marking the content with personalised display;

(ii) in providing e-commerce services, permit opt out from personalised display;

(iii) in providing news push notifications, provide convenient options to stop or turn off personalised display and options to delete or anonymise the relevant personal information; and

(iv) allow personal information subjects to manage the personal information used for personalised display and adjust the relevance of personalised display.

Automated decision-making

The new regime implements extra safeguards to protect personal information subjects in relation to automated-decision making. Personal information controllers are required to conduct personal information security impact assessments before using any automated decision–making function and periodically thereafter and, based on the results, implement effective measures to protect personal information. Personal information subjects must be given channels to object to or contest any automated decision and require human override.

V. Third-party processing

Enhanced obligations and liabilities of personal information controllers

Under the new regime, restrictions on the flow of data will be eased by removing the prohibition on sharing or transferring personal information. However, personal information controllers will be subject to new responsibilities to supervise third parties that process personal information obtained from them.

In particular, where a third party processes personal information on a personal information controller's behalf or the information is shared with or transferred to the third party, the personal information controller must ensure that the third party does not breach any laws or regulations nor the agreement between them. If there is a breach, the personal information controller must immediately require the third party to cease processing the data, take remedial measures, control or eliminate the security risks and, if necessary, terminate the business relationship with third party and require it to promptly delete the personal information.

In the event of a security incident arising out of sharing or transferring personal information, the personal information controller will be liable for any harm to the rights and interests of the personal information subjects. In the case of joint-controllers, the personal information controller must inform the personal information subjects of the identity of the third-party joint controller and their respective responsibilities and obligations. Otherwise, the personal information controller will be liable for any personal information security breach caused by the third-party joint controller.

Integration of third-party products and services

The revised Specification contemplates the scenario where a third party product or service that collects personal information is integrated into a personal information controller's own product or services. Examples include third-party products or services embedded by way of programmatic tools such as java-script, application programming interfaces, algorithms software development kits (SDK), and mini-programs. In such cases, personal information controllers are required to implement management systems, work process and, if necessary, security assessments for the integration. The security responsibilities and measures should be set out in a contract with the third party, with the personal information controller supervising and auditing compliance and keeping relevant management records. The products or services should be marked as being provided by a third party. The third party must obtain the consent of the personal information subjects and implement complaint handling mechanisms.

VI. Processing records

The amendments require the personal information controller to maintain records of its processing activities. These should contain information on aspects such as the type and source of the personal information; the purposes, use, public disclosure and international transfer of the personal information; and the systems and personnel involved in processing the personal information.

VII. Other important changes

Lower requirement for notifying data breaches

Under the new regime, personal information controllers are required to notify personal information subjects of a data breach incident only if it may cause serious harm to their legal rights and interests, for instance if there is a leak of sensitive personal information. Currently, all data breach incidents need to be communicated to the personal information subjects.

Data protection officer

The revised Specification requires that the data protection officer (**DPO**) should have relevant management and personal information protection expertise. The DPO is

required to participate in key decision-making processes relevant to personal information activities and report directly to those in charge of the organisation.

The scope of companies required to appoint a DPO is being modified. A personal information controller will be required to designate a DPO if it processes or expects to process in a 12 month-period the personal information of over 1 million personal information subjects (currently 500,000). In addition, as a new requirement, a DPO is also required where the sensitive personal information of over 100,000 personal information subjects is processed.

New responsibilities for DPOs have been added including the obligation to prepare and supervise implementing personal information protection work plans; and to provide advice and supervise mitigation and rectification of security risks. DPOs are also required to deal with complaints and the supervisory and administrative authorities in the event of issues.

Personal information controllers are required to provide the necessary support to ensure that the DPO is able to perform its duties independently.

Personal information security engineering

The new regime introduces the concept of personal information security engineering which requires personal information controllers to take into account personal information protection throughout the process of developing their products and services. This is similar to data protection by design under the GDPR. Draft guidelines on personal information security engineering were published in July 2019 for pubic consultation.

Personal biometric information

The revised Specification lays down additional safeguards to protect personal biometric information. Personal information controllers must obtain separate consent to collect personal biometric information after having notified the personal information subject of the purpose, means, scope and storage time limits of the processing.

Personal biometric information must be separately stored and segregated from personal identity information. As a general principle, raw personal biometric information (eg samples and images) should not be stored. Personal information controllers may, however, take the following measures:

(i) store only summary information (which cannot be used to trace the original information); and

(ii) use personal biometric information to identify or verify identification at the point of collection after which the original image must be deleted.

Personal biometric information should, in general, not be shared or transferred to a third party. Where this is necessary, the personal information controller must obtain explicit consent from the personal information subjects after disclosing the purpose, types of personal biometric information and the identity and security protection capabilities of the receivers.

Personal information security impact assessment

The new regime requires personal information controllers to conduct personal information security impact assessments in a number of circumstances. Apart from scenarios like pooling and convergence of personal information and automated decision-making discussed above, a personal information controller should also conduct such an assessment before launching a product or service or if the functions of its product or service have changed significantly. However, the existing requirement for periodical assessments (at least once a year) will be removed.

Back

OUR OBSERVATIONS

I. Focus on consent

A key feature of the amendments to the regime is the focus on consent. The revised Specification defines consent and amends the definition of explicit consent. The new definition of consent, which includes passive acts, may on the face of it have lessened the requirement and made it susceptible to abuse by personal information controllers. However, the revised Specification places great emphasis on ensuring that consent is freely given in the context of a service or product involving processing for multiple business functions, and proposes a mechanism for achieving this in Appendix C. This will provide useful guidance to personal information controllers in an area where personal information subjects are currently often not given the opportunity to give separate consent for respective personal information processing business functions.

II. Targeting new technologies

The revised Specification dedicates a number of sections to regulating profiling technologies prevalent in the market, including the use of personalised display, automated decision-making, and pooling and convergence of personal information from different sources. Detailed requirements are being introduced on the integration of third-party products and services commonly seen on webpages and mobile apps. Additionally, special protection is being afforded to personal biometric information throughout the processing process, which is widely used by personal information controllers using artificial technology. These sections are particularly relevant to internet companies and high-tech companies that employ these technologies to process large volumes of personal information.

III. New compliance measures

Notably, the new regime introduces regulations covering personal information security engineering. With the introduction of the revised Specification, a form of “protection by design” will be implemented soon. The maintenance of records of personal information processing activities is also a new requirement, which will help personal information controllers to monitor their own processing activities as well as assist the regulatory authorities in supervision.

Back

FIND OUT MORE

WEBSITE

OUR EXPERTISE

OUR PEOPLE

WHERE WE WORK

HUBS

BLOGS

LATEST THINKING

Global perspectives and local insights from our legal experts

READ MORE

STAY CONNECTED

KEY CONTACTS

Nanda Lau
Partner
Mainland China
+86 21 2322 2117
Email

Gavin Guo
International Partner, Kewei
Mainland China
+86 21 2322 2171
Email

James Gong
Of Counsel
Mainland China
+86 10 6535 5106
Email